FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1473462-000

Total Deleted Page(s) = 65
Page 4 ~ Duplicate;
Page 7 ~ Duplicate;
Page 23 ~ Duplicate;
Page 24 ~ Duplicate;
Page 25 ~ Duplicate;
Page 27 ~ Duplicate;
Page 29 ~ Duplicate;
Page 31 ~ Duplicate;
Page 37 ~ Duplicate;
Page 43 ~ Duplicate;
Page 45 ~ Duplicate;
Page 46 ~ Duplicate;
Page 52 ~ Duplicate;
Page 53 ~ Duplicate;
Page 55 ~ Duplicate;
Page 56 ~ Duplicate;
Page 58 ~ Duplicate;
Page 59 ~ Duplicate;
Page 61 ~ Duplicate;
Page 62 ~ Duplicate;
Page 64 ~ Duplicate;
Page 65 ~ Duplicate;
Page 67 ~ Duplicate;
Page 68 ~ Duplicate;
Page 70 ~ Duplicate;
Page 71 ~ Duplicate;
Page 73 ~ Duplicate;
Page 74 ~ Duplicate;
Page 76 ~ Duplicate;
Page 77 ~ Duplicate;
Page 79 ~ Duplicate;
Page 80 ~ Duplicate;
Page 82 ~ Duplicate;
Page 83 ~ Duplicate;
Page 85 ~ Duplicate;
Page 87 ~ Duplicate;
Page 89 ~ Duplicate;
Page 90 ~ Duplicate;
Page 91 ~ b3; b6; b7C; b7E;
Page 97 ~ Duplicate;
Page 98 ~ Duplicate;
Page 102 ~ Duplicate;
Page 103 ~ Duplicate;
Page 104 ~ Duplicate;
Page 105 ~ Duplicate;
Page 106 ~ Duplicate;
Page 107 ~ Duplicate;
Page 109 ~ Duplicate;
Page 110 ~ Duplicate;
Page 114 ~ Duplicate;
Page 115 ~ Duplicate;
Page 116 ~ Duplicate;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 119 ~ Duplicate;
Page 121 ~ Duplicate;
Page 122 ~ Duplicate;
Page 124 ~ Duplicate;
Page 125 ~ Duplicate;
Page 129 ~ Duplicate;
Page 130 ~ Duplicate;
Page 131 ~ Duplicate;
Page 132 ~ Duplicate;
Page 133 ~ Duplicate;
Page 134 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXX

X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/29/2001

[redacted] of Network Consulting contracted to World View Resources, Inc., 1724 Franklin Street, Henderson, Kentucky 42420-5208, telephone number [redacted] cell phone [redacted] was telephonically interviewed at his place of employment. The identity of the interviewing Agent was previously established by [redacted] from a previous investigation. Through the telephonic interview and use of e-mail, the following information was obtained: b6 b7C

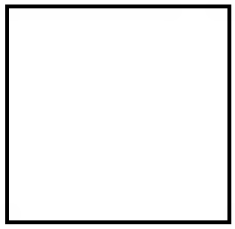
[redacted] stated during the night of 05/07/2001, the web site of World View Resources was replaced by a web page reading, "fuck USA Government fuck PoizonBox contact:sysadmcn@yahoo.com.cn". [redacted] stated damage was minimal and the original web page was retrieved from back-up in case of this type of an attack. b6 b7C

Upon writer's request, [redacted] e-mailed several pages of information to writer.

Investigation on 05/08/2001 at Louisville, Kentucky (telephonically)

File [redacted] Date dictated 05/29/2001 b3 b6 b7C

by SA [redacted] b7E



b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/29/2001

[redacted] b6 b7C

[redacted] date of birth [redacted] Social Security Account Number [redacted] telephone number [redacted] was interviewed at his place of employment, Morgan & Pottinger Law Firm, 601 West Main St., Louisville, Kentucky 40202, telephone number [redacted] The identity of the interviewing Agent was previously established by [redacted] from a previous investigation. On 05/22/2001, writer telephonically interviewed [redacted] at his place of employment. Through the use of e-mail and follow-up interview on 05/23/2001, the following information was obtained:

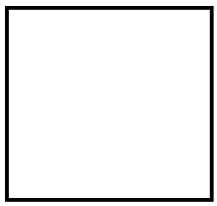
[redacted] explained four of Morgan & Pottinger web sites had been compromised and defaced within twenty minutes of each other the night of 05/09/2001. The web pages had been replaced by a web page stating "fuck USA Government fuck PoizonBox contact:sysadmcn@yahoo.com.cn". [redacted] tracked the IP address to a Korean address of 210.179.217.2. b6 b7C

After [redacted] contacted writer on 05/10/2001, writer advised [redacted] to obtain patches per the NIPC advisory. During the interview on 05/23/2001, [redacted] stated these patches worked and that Morgan & Pottinger did have some holes that [redacted] was unaware of. [redacted] stated the systems at Morgan & Pottinger still get probed approximately two times per day. [redacted] estimates the damage to the web pages to be approximately $1500. [redacted] provided the interviewing Agent with several hard copies of the logs. b6 b7C

Investigation on 05/23/2001 at Louisville, Kentucky

File [redacted] Date dictated 05/29/2001 b3 b6 b7C b7E

by SA [redacted]



b3
b6
b7C
b7E

(Rev. 08-28-2000)

IPIC

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 06/13/2001

To: Chicago Attn: SA [redacted] b3 b6 b7C b7E

From: Louisville
Squad 5
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

Title: Hacker/Honker Union of China
Illinois Secretary of State
Intrusion
04/03/2001

Synopsis: To report on interviews conducted per lead from Chicago.

Enclosures: Enclosed for Chicago are the following:

1) One original and one copy of FD-302's for interviews of [redacted] b6 b7C

2) logs provided to FBI Louisville from Morgan & Pottinger,

3) log information provided to FBI Louisville from World View Resources via e-mail,

4) log information provided to FBI Louisville from Choice Systems,

5) NIPC Cyber Incident Report Form submitted by Covington Board of Education.

Details: Per lead sent from Chicago Division concerning captioned matter, writer was able to identify three companies who reported being targets of the Chinese web page defacement attacks. Writer sent a communication to all INFRAGARD members and several individuals on a local office alert list requesting any and all victims of captioned matter to contact the FBI Louisville office immediately.

[redacted] b3 b7E

b3
b7E

Two companies responded with positive information and were interviewed immediately. The FD-302's of those interviews are included.

During the course of investigating another lead from another field office, a third company was discovered as being a victim of the web page attack. This company is Choice Systems.

A fourth organization, Covington Board of Education, responded via the NIPC Cyber Incident report Form found on the NIPC web page. This report was forwarded to writer. A voice mail message was left for the contact several times, but no response was ever realized. Contact information for the Covington Board of Education is being forwarded to Chicago with this communication.

In summary, all three companies report very little expense and describe the loss as time lost in reconfiguring the web pages back to their normal status.

Louisville considers this lead covered.

LEAD (s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

FD-542 (Rev. 11-02-1999)

Chicago

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/30/2001

To: Portland **Attn:** [redacted]

From: Portland
Squad 4
Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HACKER/HONKER UNION OF CHINA
CHICAGO SYSTEMS GROUP - VICTIM
INTRUSION

Synopsis: To claim stat for identification of compromised sites.

Details: On May 4, 2001 and May 17, 2001, Portland provided Chicago with information related to 15 compromised servers identified by Portland during its investigation of Chinese based web page defacements. (See serials 4 and 22 respectively in the above case)

[redacted]

b3
b7E

To: Portland From: Portland
Re: [redacted] 05/30/2001 b3 b7E

Accomplishment Information:

Number: 15
Type: NIPCIP COMPROMISED SITE'S IDENTIFIED AND NOTIFIED
ITU: AGENT INTERVIEW
ITU: LIAISON WITHIN FBI
Claimed By:
SSN: [redacted] b6 b7C
Name:
Squad: 4

♦♦

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2001

To: Chicago **Attn:** Evidence Custodian Technician
SA [redacted] b3 b6 b7C b7E

From: Richmond
Squad 7, Roanoke RA
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: UNSUBS;
HONKERS UNION OF CHINA;
INFINITY TEL-DATA, INC.;
ET AL. - VICTIM
COMPUTER INTRUSION

Synopsis: Sound Stage, Roanoke, VA, experienced a computer network intrusion traced back to a site(s) in China. No significant damage reported. Information provided to CG for review and to determine its relevancy with regard to captioned investigation.

Package Copy: One "CD" and printout of a computer log and computer file left on the network server of Sound Stage, 103 8th Street, Southeast, Roanoke, Va. 24013, [redacted] for transmittal to CG. b6 b7C

Details: [redacted] Sound Stage, contacted the Roanoke, RA, Richmond Division, to advise that a file inserted into their computer system is believed to have originated in China. No damage was done to Sound Stage's system, and the file was removed and the "holes" were successfully patched. [redacted] advised he was unsure as to when the initial intrusion occurred, but the computer logs will show the date upon which the file was discovered and extracted/removed. Sound Stage is unaware of any previous problems regarding the site in China, and has not had any further difficulties since that time. [redacted] advised that no significant monetary damages were caused by this event.

[redacted] b3 b7E

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL.

Review enclosed material for its relevancy and possible inclusion into ongoing captioned investigation.

♦♦

(Rev. 08-28-2000)

Honker Union. cc

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/29/2001

To: Chicago **Attn:** SA [redacted] b3 b6 b7C b7E

Philadelphia
Williamsport RA
Contact: SA [redacted] 570-329-5328

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

Title: Hacker Honker Union of China;
Illinois Secretary of State;
04/03/2001;
Intrusion

Synopsis: Three complaints received by Williamsport RA (Philadelphia Division) in reference to above captioned case.

Reference: [redacted] b3 b7E

Details: Three complaints have been telephonically received by the Williamsport RA in reference to the Honker Union of China hacking case.

Complaint #1 (Reported 05/07/2001)

The complainant [redacted] 800 West Fourth Street, Williamsport, PA, telephone number 570-323-1010 ext. [redacted] is the [redacted] for REGSCAN, INC., an electronic publishing and Internet web-site developer located in Williamsport, PA. The complainant advised that one of REGSCAN's computer systems was hacked into through port 80 using a vulnerability in the Solaris operating system. The attack occurred Saturday, May 5, 2001 from approximately 11:15 a.m. to 12:15 p.m. b6 b7C

Specifically, the sadmind/IIS worm is suspected in the attack, based on information provided to REGSCAN by the CERT advisory staff at Carnegie Mellon University. The worm takes advantage of a two-year old buffer overflow vulnerability in the Solstice sadmind program. Once the system is compromised, the hacker utilizes a seven-month old vulnerability in the IIS system. The complainant advised that the REGSCAN computer system [redacted] b3 b7E

 b3 b7E

did not have the latest IIS patch installed on the operating system.

After the system was hacked, the attacker modified the REGSCAN web-site by placing the message "Fuck the USA Government, Fuck Poison Box" on the home page. The IIS log files revealed the offender with an IP address of 210.77.147.216. [redacted] b7E

[redacted]

[redacted] b7E

Based on the context of the disparaging message left on the web-site, it is believed that the attack may have been one of several attacks occurring in recent days between Chinese and U.S. hacker groups, in the aftermath of the collision between an U.S. Navy Intelligence plane and a Chinese fighter jet. "Poizon Box" is a known U.S. hacking group, made reference to in a portion of the disparaging message. It is believed that the attack most likely originated in China.

No data was lost in the attack, and minimal time was spent on repairing the web page and installing the IIS patch.

Complaint #2 (Reported 05/03/2001)

The complainant [redacted] SEDA-COG, RR1 Box 372, Lewisburg, PA, Telephone number 570-524-4491, ext. [redacted] is a [redacted] at Susquehanna Economic Development Association - Council of Governments(SEDA-COG). SEDA-COG is federally funded through various federal grants. The complainant advised that an unknown hacker compromised their computer server on 05/02/01 at approximately 12:15 P.M. The hacker modified the the SEDA-COG web-site home page with derogatory information. b6 b7C

Specifically, the hacker left the message "Fuck USA Government" and "Fuck PoizonBOx" on the web site. The complainant advised that SEDA-COG utilizes Microsoft Servers with all the current patches installed.

A review of the appropriate log files revealed IP Address 210.230.128.198 logged at 12:08:59 P.M. on 05/02/01. The IP address returns to Japan Network Information Center, Fuundo Building, 3F, 1-2 Kanda-Ogawamachi, Chiyoda-ku, Tokyo 101-0052, Japan, an Internet Service Provider in Japan.

 b3 b7E

The complainant estimates the attack caused four staff members to work two days to bring the web-site back online. No data loss occurred as a result of the hack.

Based on the information from the complainant, the Williamsport Resident Agency believes the attack is one of many conducted by various Chinese hackers in retaliation for the collision between a U.S. Navy Surveillance plane and a Chinese jet fighter several weeks ago,

Note: On May 10, 2001, a news brief on AP Wire indicated the following:

"A self-styled alliance of Chinese computer hackers has called a halt to attacks on U.S. Web sites, after claiming to have broken into more than 1,000 sites. The group that calls itself the "Hongke Union" thanked hackers for taking part in the campaign against U.S. wen sites, but said it would not be connected to any further attacks. Chinese hackers declared a weeklong war on U.S. sites, from April 30 to May 7 (2001), after a U.S. Navy spy plane collided with a Chinese fighter jet setting off a diplomatic standoff. The fighter pilot was killed in the April 1 collision. Hackers attacked the White House Web site on May 4, leaving it completely blocked or difficult to access for about six hours."

Complaint #3 (Reported 05/18/2001)

The complainant [redacted] Brodart Company, 500 Arch Street, Williamsport, PA 17705, telephone number 570-326-2461, etx. [redacted] e-mail: [redacted] is a [redacted] with Brodart Company in Williamsport, PA. b6 b7C

Brodart had two computer hacking attacks, one on 05/04/2001 with a logged IP address of 210.59.251.135, and the second on 05/06/2001 with a logged IP address of 137.140.8.104. The attackers modified a web page on a "non-live" server which read, "Fuck the USA Government, Fuck Poizonbox."

Brodart runs the Windows 2000 operating system on their servers. [redacted] advised that at the time of the attack, service pack 2 was not installed, which made the servers vulnerable to the Sadmind worm attack. b6 b7C

[redacted] advised that the 05/06/2001 attack was relayed through a Sun Solaris system operated by a State University of New York(SUNY) professor in New Paultz, NY. Brodart personnel

b3
b6
b7C
b7E

contacted [redacted] (telephone number [redacted]) at SUNY to advise them of the route-thru attack.

In all three complaints, the complainants were advised to maintain their log files and web page modifications, as evidence, should the FBI prosecute any case in this matter.

To: Chicago Fr[redacted] Philadelphia b3
Re: [redacted] 05/29/2001 b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO

For information, read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/25/2001

[redacted] date of birth [redacted] Social Security Account Number [redacted] address [redacted] telephone number (cellular) [redacted] was contacted by Special Agent (SA) [redacted] Federal Bureau of Investigation (FBI), St. Louis Division. After being advised of the identity of the interviewing Agent, [redacted] provided the following information: b6 b7C

[redacted] a web host development business with the financial assistance from [redacted] b6 b7C

Two of [redacted] computer servers were attacked by hackers believed to be from China. [redacted] main server was partially owned by a third party, Lamont Development Group. [redacted] provided [redacted] name as a point of contact Lamont. The Lamont Development Group actually purchased the equipment and it was being maintained at the Cybercon Company, 210 North Tucker Street, St. Louis, Missouri.

[redacted] second server, primarily developmental and testing was solely owned and operated by Electranet USA, [redacted] business, also known as Electric Man Internet Services. b6 b7C

On Sunday, May 5, 2001, at approximately 9:00 A.M., [redacted] discovered that someone had attacked his server. [redacted] had been working on the server on Saturday evening, May 4, 2001, and finished his work about 8:00 P.M. Upon re-entering the server on Sunday, [redacted] discovered the intrusion.

One of [redacted] clients had their web page replaced with a Chinese flag, and music (possibly the Chinese national anthem) and a message about President Bush being a murderer along with other remarks. [redacted] had saved all of the web defacement images, but all of the web site files had been deleted by the hackers. b6 b7C

[redacted] had written all of the code for the web sites and would be able to replace web page. However, [redacted] discovered the hackers had erased any activity in the log files of their

---

Investigation on 05/22/2001 at St. Louis, Missouri b3

File # [redacted] Date dictated 05/15/2001 b6 b7C

by SA [redacted] b7E

136[redacted]06.302

intrusion. [redacted] had unplugged the Internet access to the server until he could address the problem.

[redacted] had been remotely accessing the second server(used for development and testing) on Sunday, May 5, 2001 and on Monday, May 6, 2001 until about 1:00 P.M., at which time he stopped to run an errand. b6 b7C

Upon attempting to access the second server again, [redacted] discovered the management console counselor for passwords had been deleted. The event logs, service logs, a new directory called "Fuck You" and other directories had been recreated by the hackers.

The second server had been manipulated so that passwords could not be changed by [redacted] or other users. In the default directory, there were web pages with slanderous remarks. There was also an executable file, "sr.exe", which showed that it was modified on May 6, 2001 at 2:02 P.M. The hackers had also removed the file needed to reboot the system. [redacted] was concerned about how the hackers had been able to obtain system-level access without using passwords. b6 b7C

All of [redacted] fifty-three customer web pages were affected by the attack. Some of the customers had contacted [redacted] about their web pages being down. [redacted] told his customers that he was having a security problem and was addressing it. b6 b7C

[redacted] started his business in August of 2000. [redacted] used to work for an Internet Service Provider (ISP) that went out of business. [redacted] started his own business and began recruiting back some of customers of the failed ISP.

[redacted] showed SA [redacted] the web page defacement. The defacement was mostly black with red lettering and the words "Honker Union of China" "Hacked by red freedom" "USA = Nazi" "Bush = Murderer" "Beat down imperialism of America". b6 b7C

[redacted] provided a listing of the files which had been deleted from a back-up copy which he had. [redacted] also provided passwords for both of the servers that had been attacked.

[redacted] estimated that the attack had cost him $16,633.00 in business and $11,583.00 in lost time to make the necessary repairs for a total of $28,216.00

[redacted]

b3
b6
b7C
b7E

Both servers were taken by SA [redacted] for a forensic examination to be performed by the St. Louis Division. [redacted] was provided a FD-597, Receipt for Property form, from SA [redacted] for the following two servers:

b6
b7C

1) Compaq Proliant ML370 server

2) IBM Clone web server, Creative Labs, containing a DVD ROM drive in the CD Bay

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/19/2001

[redacted] Mary Institute and Saint Louis Country Day School(MICDS), was contacted by SA [redacted] Federal Bureau of Investigation, St. Louis Division. After being advised the identity of the interviewing agent, [redacted] provided the following information: b6 b7C

[redacted] had e-mailed the St. Louis Division with a request for assistance with a web page attack at MICDS. SA [redacted] had telephonically contacted [redacted] and scheduled an appointment to pickup the computer system logs from the attack.

On May 7 and May 10, 2001, a public web server at Mary Institute and Saint Louis Country Day School(MICDS) was attacked. [redacted] was notified by the Technology Department about the defacement on 5/7 and by the Business Department on 5/10. b6 b7C

The server was running Windows 2000, Service Pack 1 and Internet Information Services (IIS) 5.0. The DNS(Domain Name Server) was mail.micds.org. [redacted] applied new patches to fix the problem after researching the attack on CERT(Computer Emergency Response Team) web page.

The attack shutdown a web page and replaced the text with the message, "Fuck USA Government, Fuck PoizonBOx, contact sysadmcn@yahoo.com.cn"

[redacted] attempted to send e-mails to the hosts, which appeared on the logs, but all attempts at communication bounced. [redacted] deleted all the files which were modified and redirected the web page. [redacted] then recreated the web page. b6 b7C

[redacted] supplied a floppy diskette to SA [redacted] with the log activities from the attack.

Investigation on 05/21/2001 at St Louis

File # [redacted] Date dictated

by SA [redacted] b3 b6 b7C b7E

170[redacted]01.302

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/19/2001

[redacted] Southwestern Bell Cellular, Date of Birth [redacted] telephone number [redacted] telephonically contacted the St. Louis Division and talked with SA [redacted] scheduled a time and date to meet an discuss a web page defacement at Washington University, Psychology Department where [redacted] agreed to meet at the St. Louis Division Office, 2222 Market Street, St. Louis, Missouri. b6 b7C

[redacted] was contracted to build a database for nationwide research by Washington University, Psychology Department in September 2000. [redacted] obtained his graduate degree in Computer Science from Washington University. b6 b7C

The database was to be accessible to other researchers throughout the nation. The web page for the database was defaced by unknown attackers who replaced the web page with the text,"Fuck USA Government, Fuck PoizonBOx, contactsysadmcn@yahoo.com.cn".

[redacted] advised SA [redacted] that he would e-mail the system logs to SA [redacted] the next time he was physically at the server. [redacted] advised the GET command was utilized on Port 80 to gain entry into the database server. b6 b7C

[redacted] had already traced two of the IP (Internet Protocol) addresses back to China and Brazil. The China IP address was 210.52.149.171 and the Brazil IP address was 200.199.223.150.

 b3 b6 b7C b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2001

[redacted] of Science and Math Tutoring, located at 18 Arbor Road, St. Louis, Missouri 63132, telephone number [redacted] was telephonically contacted by Special Agent (SA) [redacted] Federal Bureau of Investigation (FBI), St. Louis Division. After being advised of the identity of the interviewing Agent, [redacted] provided the following information about a web site attack: b6 b7C

[redacted] had submitted an incident report the National Infrastructure Protection Center (NIPC) about a web page defacement on May 12, 2001. The attack took place approximately May 5, 2001.

The attack was similar to other web site defacements by the Honker Union of China. The attacks take over the web site and display a message that states "Fuck USA Government, fuck PoizonBOx, contactsysadmcn@yahoo.com.cn". The screen is normally black and the letters of the text are red.

[redacted] contacted his systems engineer technician, [redacted] of Wareforce, telephone number [redacted] performed all of the patch updates to help secure the system from future similar exploits. [redacted] paid $100.00 for the services of [redacted] b6 b7C

[redacted] server was not used for any type of tutoring, but rather for advertising of the science and math tutoring business. b6 b7C

[redacted] opined that the attack might possibly be the Chinese since an IP address from the source of the attack originated from China.

[redacted] suggested that SA [redacted] contact [redacted] to discuss some of the technical questions of the attack.

Investigation on 06/14/2001 at St. Louis (telephonically)

File # [redacted] Date dictated 06/13/2001 b3 b6 b7C b7E

by SA [redacted]

165 [redacted] 01.302

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

Approved By: [redacted]

Drafted By: [redacted]

b3
b6
b7C
b7E

Case ID #: [redacted]

Title: Subject: HONKER UNION OF CHINA
Victim: Math & Science Tutoring
Type: Computer Intrusion (Web Page Defacement)
Date: 05/05/2001

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED: 05/10/2001

CASE CLOSED: 06/11/2001 (Referred to Chicago Division)
☐ No action due to state/local prosecution
(Name/Number:_____)
☐ USA declination
☐ Referred to Another Federal Agency
(Name/Number:_____)
☐ Placed in unaddressed work
x Closed administratively
☐ Conviction

COORDINATION: FBI Field Office St. Louis Division
Government Agency _____
Private Corporation _____

VICTIM

Company name/Government agency: Math & Science Tutoring
Address/location: 18 Arbor Road, St. Louis, MO 63132
Purpose of System: Advertising Tutoring Business
Highest classification of information stored in system: N/A

UPLOADED TO ACS/ECF
BY SL, 6/20/01 [redacted]

b3
b6
b7C
b7E

16[redacted]03.oth

[redacted]

To: Counterterrori[redacted] From: Washington Field[redacted] b3 b7E
Re: [redacted] Date: 06/12/2001

System Data:

Hardware/configuration (CPU): Compaq Proliant 1600 (rack mount)
Operating System: Windows NT 4.0
Software: _____

Security Features:

Security Software Installed: ☐ yes (identify _____) X no
Logon Warning Banner: ☐ yes X no

INTRUSION INFORMATION

Access for intrusion: X Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Internet address: dynamic
Network name: _____

Method:

Technique(s) used in intrusion: ISS/Sadmind Exploit (list provided)

Path of intrusion:
addresses: 1. 217.0.35.89 2. _____ 3. _____
country: 1. _____ 2. _____ 3. _____
facility: 1. _____ 2. _____ 3. _____

Subject:

Age: _____ Race: _____
Sex:: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: HONKER UNION OF CHINA
Employer: _____
Known Accomplices: _____
Equipment used: _____
Hardware/configuration (CPU): _____
Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ yes X no
Estimated number of computers affected: 1
Estimated dollar loss to date: $100 Service Charge

To: Counterterrori[redacted] From: Washington Field [redacted]
Re: [redacted] Date: 06/12/2001 b3 b7E

Category of Crime:

Impairment:
- x Malicious code inserted
- ☐ Denial of service
- ☐ Destruction of information/software
- x Modification of information/software

Theft of Information:
- ☐ Classified information compromised
- ☐ Unclassified information compromised
- ☐ Passwords obtained
- ☐ Computer processing time obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

Intrusion:
- x Unauthorized access
- ☐ Exceeding authorized access

REMARKS

On May 5, 2001, Science and Math Tutoring had their web page defaced by unknown attackers. [redacted] hired Wareforce, a computer security company, to fix the problem and install new patches. b6 b7C

Wareforce sent [redacted] to Science and Math Tutoring to repair any damage and install the patches to prevent future attacks using the same exploit. [redacted] has performed services at Science and Math Tutoring prior this service call. [redacted] updated the computer system with latest Windows NT patches.

[redacted] suggested to [redacted] that a report be submitted to the FBI regarding the incident. [redacted] completed the National Infrastructure Protection Center Report and facsimiled the report to the Watch and Warning Unit located in Washington, D.C. on May 12, 2001. The report was later forwarded to the St. Louis Division on May 22, 2001.

The web defacement had the same text as many other businesses in the St. Louis area. The message stated, "Fuck USA Government, fuck PoizonBOx, contact sysadmcn@yahoo.com.cn"

[redacted] was not familiar with his computer system enough to answer some of the questions needed for this form so [redacted] advised SA [redacted] to telephonically contact [redacted] and ask him the technical questions. SA [redacted] asked [redacted] if [redacted] would charge Science and Math Tutoring a fee for answering technical questions about their computer system. [redacted] advised that [redacted] was very nice and he should not have any problems answering the technical questions. b6 b7C

To: Counterterrori[redacted] From: Washington Field[redacted]
Re: [redacted] Date: 06/12/2001

b3
b7E

On June 12, 2001, SA [redacted] telephonically contacted [redacted] about [redacted] computer system. [redacted] provided the technical information about the system such as CPU, Operating system. [redacted] advised that the system had a service pack 3 or 4 on it and he upgraded to service pack 6 to prevent the same exploit from occurring again.

b6
b7C

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/2001

[redacted] for Wareforce, Computer Security Technician, telephone number [redacted], was telephonically contacted by [redacted] Federal Bureau of Investigation (FBI), St. Louis Division. After being advised the identity of the interviewing Agent, [redacted] provided the following information: b6 b7C

[redacted] was contracted by [redacted] Science and Math Tutoring located at 18 Arbor Road, St. Louis, Missouri, to secure his computer system after a web page defacement. b6 b7C

[redacted] suggested that [redacted] contact the National Infrastructure Protection Center (NIPC) to report the attack. [redacted] had heard from other computer technicians this was the proper procedure for these types of web page attacks.

SA [redacted] asked [redacted] about some of the hardware and software on [redacted] system. [redacted] stated that [redacted] was using a Compaq Proliant 1600 rack-mount running Windows NT 4.0. [redacted] had service pack 3 or 4 on the system, which [redacted] updated to service pack 6. b6 b7C

[redacted] stated that [redacted] was using a dynamic IP address at the current time. [redacted] also stated that a vulnerability in Internet Information Services (IIS) was what was exploited by the attacker(s).

SA [redacted] about the logs. [redacted] stated that [redacted] should be able to go into his system and retrieve the logs and e-mail those to SA [redacted] b6 b7C

[redacted] assisted [redacted] in completing the incident report for NIPC. [redacted] wrote on the bottom of page 3 where he had saved the logs from the attack had written at the bottom of page 3 that he had placed log files from the hack in D:\hack\logs\. [redacted] suggested that SA [redacted] have [redacted] e-mail the logs to SA [redacted]

Investigation on 06/14/2001 at St. Louis (telephonically)

File # [redacted] Date dictated 06/13/2001 b3 b6 b7C b7E

by SA [redacted]

165 [redacted] 02.302

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/19/2001

To: Chicago **Attn:** Squad IP/C
SA [redacted]

St. Louis

[redacted]

From: St. Louis
Squad 3
Contact: SA [redacted] 314-589-2719

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Hacker/Honker Union of China
Illinois Secretary of State
Intrusion
04/03/2001

Synopsis: Submit all case related documents from the St. Louis Division on above captioned matter.

Reference: [redacted] b3 b7E

Enclosure(s): Enclosed for the Chicago Division are the following case documents from victims in the St. Louis Division:

1. Electranet- One original and one copy of FD-302 of interview of victim, [redacted] one 1-A envelope containing notes of SA [redacted] and FD-597 for receipt of two servers, one 1-A envelope containing FD-597 for return of two servers, copy of FD-801. b6 b7C

2. City of St. Louis, Water Division - One original and one copy of FD-302 interview of [redacted] one original and one copy of FD-302 of [redacted] faxing documents to St. Louis Division, one 1-A envelope containing floppy diskette with logs, one 1-A envelope containing notes of SA [redacted] one copy of documents faxed to St. Louis Division, one copy of FD-801.

UPLOADED TO ACS/ECE
BY SL 6/20/01 [redacted]

[redacted] b3 b6 b7C b7E

 b3 b7E

3. Mary Institute and Saint Louis Country Day School (MICDS) - One original and one copy of FD-302 interview of [redacted] at MICDS, one copy of summary from [redacted] one copy of e-mail message to st.louis@fbi.gov from [redacted] one 1-A envelope containing floppy disk with logs, copy of FD-801. b6 b7C

4. St. Louis Bridge Company - One copy and one original of FD-302 interview of [redacted] one 1-A envelope of zip disk with logs, hacker tools and NIPC incident report, 13 pages of IP address Whois lookups from [redacted] copy of Incident Report and letter submitted by [redacted] copy of FD-801.

5. Washington University - One original and one copy of FD-302 interview of [redacted] original logs, e-mail message from [redacted] to SA [redacted] copy of FD-801. b6 b7C

6. Science and Math Tutoring - One copy and one original of two FD-302's of interviews of [redacted] and [redacted] one 1-A envelope of SA [redacted] notes, one copy of NIPC Incident Report and one copy of FD-801.

Details:

Electranet

On May 6, 2001, [redacted] Electranet, Web Host Development Company, telephonically contacted the St. Louis Division to report a web page defacement. The defacement consisted of the Red China flag, music believed to be the Chinese National anthem, and the text,"Honker Union of China" "Hacked by red freedom" "USA=Nazi" "Bush=Murderer""Beat down imperialism of America". [redacted] main server which was hosting fifty-three customer sites was attacked on 05.06/2001. [redacted] suffered another attack on his development/testing server on 05/07/2001, [redacted] system was compromised and several files and directories were deleted by the attackers and passwords were changed preventing access by [redacted] or other users. [redacted] could not produce any logs on the attack. b6 b7C

City of St. Louis Water Division

On May 14, 2001, [redacted] City of St. Louis Water Division telephonically contacted [redacted] Assistant Infraguard Coordinator, about a web page defacement which occurred on 05/07/2001. [redacted] faxed some documents to [redacted] which included a very brief log. SA [redacted] interviewed [redacted] and received a floppy disk with logs and html code. The defacement did not reveal the text b6 b7C

b3
b7E

which was written in the code. The text should have read, "Fuck USA Government, Fuck PoizonBOx, contactsysadmcn@yahoo.com.cn". [redacted] opined that because he does not use Outlook to view text the code did not work as designed. [redacted] was concerned about how attackers made it pass his DMZ firewall configuration without the logs documenting the activity. [redacted] used the Checkpoint Firewall-1 Software.

b6
b7C

Mary Institute and Saint Louis Country Day School

On May 7, 2001, the Mary Institute and Saint Louis Country Day School (MICDS), was attacked with web defacements. [redacted] e-mailed the St. Louis Division about the defacement. SA [redacted] contacted and received a floppy disk with a very comprehensive log history. The defacement consisted of the text (paraphrased) "F.. USA Gov.., F.. PoizonBOx, contact...cn". The text was in red with black background. [redacted] attempted to send e-mails to the origins of the IP addresses, but all attempts bounced.

b6
b7C

St. Louis Bridge Company

On May 14, 2001, the St. Louis Division received an incident report and letter (explained incident) from the NIPC Watch and Warning Unit which had been submitted by [redacted], [redacted] St. Louis Bridge Company. SA [redacted] [redacted] contacted [redacted] and received logs and IP address searches conducted by [redacted] The attackers were successful in accessing the employee Intranet and displaying the defacement. A log showed the letters HUC, which is believed to stand for Honker Union of China. The hard drive on the company's server was erased causing the system to crash. [redacted] discovered through his own investigation that his system was first breached on March 24, 2001.

b6
b7C

Washington University, Psychology Department

On May 11, 2001, the Washington University, Department of Psychology, data base server web page was defaced. The server was utilized in a research project nation wide. [redacted] of the data base server contacted the St. Louis Division. [redacted] provided logs on the defacement, which was consistent with other defacements by the Honker Union of China, (paraphrased text) "F..USA Gov..,""F..PoizonBOx.""contact...cn".

b6
b7C

Science and Math Tutoring

On May 12, 2001, an incident report was submitted to NIPC Watch and Warning Unit from [redacted] Science and Math Tutoring. The Incident Report was forwarded to SA [redacted] St. Louis Division, who telephonically contacted [redacted] server was attacked with web defacement

b6
b7C

similar to above stated cases. The defacement was as follows(paraphased)"F..USA Gov.."F..PoizonB.."contact...cn". [redacted] contacted his [redacted] who applied patches to the Windows NT system. b6 b7C

The St. Louis Division was made aware of other similar incidents of web page defacements by the above mentioned victims, however, there was not any reports or contact made by the actual victims of the attacks.

The St. Louis Division considers this lead covered unless further advised by the Chicago Division.

16[redacted]01.EC b6 b7C

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/19/2001

To: Chicago **Attn:** SA [redacted]
Squad IP/C

[redacted]

From: Newark
Squad 2/Franklin Township Resident Agency
Contact: SA [redacted] 732/805-0463 ext. 271

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) [redacted]

b3
b6
b7C
b7E

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE;
INTRUSION
04/03/2001

Synopsis: Report results of interviews of companies whose websites were defaced by captioned subject. Lead covered.

Reference: [redacted]

b3
b7E

Enclosure(s): An original and two copies of FD-302's and 1A envelopes with a 3.5" disk and original interview notes for each of the following: ADP, INC., BURNS & ROE, CELARIX, INC., DATANOMICS, EDUNEERING, INC., FINANCIAL EXECUTIVES INTERNATIONAL, JANOME-AMERICA, NOURISON, PICATINNY FEDERAL CREDIT UNION, RAO.COM, SCREENZONE MEDIA NETWORKS, SOFTWARE PLUS, INC., TRIANGLE MANUFACTURING, and US MORTGAGE CORPORATION. One FD-71 form from each of the following: EBS TECHNOLOGY and TANGLIZE, INC. One Cyber Incident Report Form from GOAMERICA COMMUNICATIONS CORP.

Details: Over the past two months, FBI Newark has received numerous reports from New Jersey companies whose web pages have been defaced with anti-American slogans and references to "PoizonBOx". The media has reported these defacements are in retaliation for the Chinese spy plane incident this past Spring. FBIHQ advised FBI Chicago was coordinating the national investigation into these incidents. Subsequently, in the referenced communication FBI Chicago set a lead for FBI Newark to conduct logical investigation of New Jersey victim companies.

Results of the requested investigations are enclosed. As all logical investigation at FBI Newark is complete, Newark considers this lead covered. However, FBI Newark will continue to forward other reports of such incidents as necessary.

♦♦

b3
b7E

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/19/2001

[redacted] ADP, Inc., ADP Boulevard, Roseland, New Jersey, telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview he provided the following information. b6 b7C

ADP is a large provider of payroll and other data processing services. Over a period of days beginning on 05/04/2001 at least three of the company's websites were defaced with anti-American slogans and references. It is believed that the pages were accessed through known vulnerabilities. The web pages were for two different business units and two different sub-business units. The business units are located in different parts of the country, however at least one set of servers is hosted in Weehawken, New Jersey and may have suffered between $75,000 and $100,000 in damages.

Additional information is being gathered by the company and will be forwarded to the FBI by another ADP employee, [redacted] in the near future. b6 b7C

ADP requested that details of this incident not be disclosed publicly.

Investigation on 5/4/2001 at Somerset, New Jersey

File # [redacted] Date dictated 06/19/2001

by SA [redacted]

b3 b6 b7C b7E

1PIC

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/18/2001

To: Oklahoma City **Attn:** SSA [redacted]
✓ Los Angeles **Attn:** SA [redacted]
✓ Chicago **Attn:** SA [redacted]

From: Oklahoma City
Squad 8
Contact: SA [redacted] 405/290-7770

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: UNSUB(S);
TUCKER TECHNOLOGIES, INC. - VICTIM;
LION INTERNET WORM VIRUS

Synopsis: To document telephone conversation with victim company.

Enclosures: 3.5" floppy disk containing "tarball" of information relating to virus, for SA [redacted]

Details: On 5/2/2001, writer was telephonically contacted by [redacted] (PROTECT IDENTITY), located at [redacted]

b6
b7C
b7D

TTI is a wireline logging business with sites located in North and South America, specifically in Brazil, Columbia, Venezuela, Trinidad, Canada, and the United States. TTI's world headquarters is located in Trinidad. TTI's North American headquarters is located in Houston, Texas. TTI's Research, Development, and Production facility is located in Tulsa, Oklahoma. All of TTI's information technology operations are run from the Tulsa site, which runs a Linux network.

TTI is hired by oil companies to gather data about oil and gas wells. TTI gathers data by lowering a wireline (a cable) into these wells.

The oil business is very competitive and TTI maintains confidential client data within their computer network.

b3
b7E

[redacted]

To: Oklahoma City From: Oklahoma City b3 b7E
Re: [redacted] 05/18/2001

At approximately 3:30 a.m. on 3/22/2001, a hacker infiltrated a TTI computer located at a subsidiary site known as Tucker Wireline Services in Calgary, Canada. The infiltration was discovered because a worker noticed that the worker's machine was slow. The worker investigated the cause by looking for the processes that were using the machine's resources.

[redacted] explained that not only was a virus/worm discovered, but it appeared that the intruder used the virus/worm to gain entry into the compromised computer. The virus/worm exploited the known vulnerabilities with daemons and compromised the computer through a root exploit. The compromised computer was running old software. Once the virus/worm installed itself, it looked for other machines to attack. The virus/worm gathered password files and shadow files and sent these files out via e-mail to 1i0nssniffer@china.com and to 1i0nip@china.com. b6 b7C b7D

The virus/worm shut down all logging, so the only tracing that TTI could do was through the aforementioned e-mail addresses.

TTI got hold of the administrator at China.com, who was located in San Francisco, California. The administrator told TTI that the actual server for China.com was located in Beijing. The administrator also told TTI that a police officer from Garden Grove Police Department, Garden Grove, California, also called to inquire about the same issue. TTI acquired the officer's name, contacted him, and ultimately discussed the intrusion with this police officer.

Concerning damages, TTI's data center was "out of commission" for two days. Thousands of dollars run through this center every day. Also, two employees were occupied full-time for these two days trying to recover/fix the network.

[redacted] does not believe the intruder obtained any proprietary information. [redacted] also thinks that this attack was a random attack and that TTI was not specifically targeted. b6 b7C b7D

[redacted] explained that TTI's network is now secure. [redacted] also explained that he has a "tarball" of all files used/discovered from the intrusion. [redacted] stated that he will cooperate in any way necessary to help authorities.

Writer performed a Sam Spade DNS check of China.com and discovered that China.com comes back to IP address 202.84.13.20. This IP address resolves to a Unix HTTP server running Apache/1.3.9.

To: Oklahoma City From: Oklahoma City
Re: [redacted] 05/18/2001

b3
b7E

Writer performed a [redacted] b7E

[redacted]

To: Oklahoma City From: Oklahoma City
Re: [redacted] 05/18/2001

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

Read and clear.

Set Lead 2: (Adm)

LOS ANGELES

AT LOS ANGELES, CA

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/14/2001

[redacted] BURNS & ROE, 800 Kinderkamack Road, Oradell, New Jersey 07649, telephone number [redacted] were interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, they provided the following information. b6 b7C

BURNS & ROE is an engineering company whose worldwide headquarters is located in Oradell, New Jersey. The company's web servers are also located in New Jersey and run WindowsNT Internet Information Server (IIS) version 4.0. Early on the morning of 5/6/2001 network personnel noticed a series of port scans which originated from IP address 210.111.144.15 which resolved to SK Telecom in South Korea. Subsequent to this scan, at approximately 9:40 a.m. on 5/6/2001, the BURNS & ROE web site, www.roe.com, was defaced. The source IP address of the defacement was also 210.111.144.15 and consisted of the following message: "fuck USA Government, fuck PoizonBox, contact:sysadmcn@yahoo.com.cn". [redacted] advised it appeared someone accessed the command shell and executed an "echo" command which allowed root access and the ability to overwrite the BURNS & ROE default page. There was no other known damage to the web site or to parts of the network. b6 b7C

Original interview notes, a 3.5" diskette containing log files provided by [redacted] and hard copies of the log files are enclosed in the attached 1A envelopes.

Investigation on 05/07/2001 at Somerset, New Jersey (telephonically) b3 b6

File # [redacted] Date dictated 5/14/2001 b7C b7E

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/14/2001

[redacted] CELARIX, INC., 1 Meadowlands Plaza, East Rutherford, New Jersey 07073, telephone number [redacted] was telephonically interviewed. After being advised of the identity of the interviewing Agent and the nature of the interview, he provided the following information. b6 b7C

CELARIX, Inc. is a company which develops web applications. [redacted] an employee, advised that at 11:00 a.m. on 5/10/2001 the company's web site, www.rateexplorer.com, was defaced. The defacement consisted of the following message "fuck USA Government, fuck PoizonBOx, contact:sysadmcn.yahoo.com.cn".

CELARIX hosts their own web site. The servers are located in New Jersey and operate using Windows NT IIS version 3.0 and Windows 2000 version 5.0. [redacted] stated the intruders were able to access the "cmd.exe" file, execute a "dir" command, gain root access, and then change the cmd.exe file name. b6 b7C

The original FD-71 and a 3.5" diskette containing the logs documenting the intrusion are enclosed in the attached 1A envelope.

Investigation on 05/10/2001 at Somerset, New Jersey (telephonically) b3

File # [redacted] Date dictated 05/14/2001 b6 b7C b7E

by SA [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/18/2001

[redacted] DATANOMICS, Inc., 200 Centennial Avenue, Suite 140, Piscataway, New Jersey 08854-3923, telephone number 732/981-0192, ext. [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, she provided the following information. b6 b7C

[redacted] had previously submitted a Cyber Threat and Computer Intrusion Incident Report to the National Infrastructure Protection Center Watch and Warning Unit. The purpose of this interview was to follow-up on the information in her report.

DATANOMICS is an information technology consulting company. On 5/8/2001 and 5/11/2001 the default files on three of their web servers were replaced with the language "Fuck the government" and "Poizonbox". The attack appeared to originate from IP address 160.227.14.65 and occurred as a result of a vulnerability in WinNT IIS 4.0. Although the servers are connected to an internal computer network, no further compromise was detected nor have there been any additional attacks since the WinNT patch was installed

Enclosed in a 1A envelope is the Cyber Threat and Computer Intrusion Incident Report submitted by [redacted] to the NIPC. b6 b7C

Investigation on 05/18/2001 at Somerset, New Jersey (telephonically) b3

File # [redacted] Date dictated 05/18/2001 b6 b7C

by SA [redacted] b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] EDUNEERING, INC., 100 Campus Drive, Suite 100, Princeton, New Jersey 08540, [redacted] was advised the identity of the interviewing agent and the nature of the investigation. [redacted] then provided the following information: b6 b7C

[redacted] said EDUNEERING runs a commercial site for FDA Training and the site was down on 5/7/01 from 6:30 am for three (3) hours. [redacted] said EDUEERING's web page was replaced with anti USA Government remarks and was part of the ongoing China-USA hacking conflict. EDUNEERING's largest clients were not able to access the site and they incurred a loss in excess of $5,000. [redacted] has not calculated an exact loss amount. As a result, [redacted] made the necessary system patches to eliminate the security holes. [redacted] was able to restore the site from backups. [redacted] reviewed an executable and batch file that was used to propagate the attack and identified an IP address, 216.205.125.115. b6 b7C

[redacted] said that he would send logs of the incident that were received by FBI Newark on May 8, 2001. A copy of the log has been placed in the file. b6 b7C

Investigation on 05/08/01 at Somerset, New Jersey (telephonically) b3 b6 b7C b7E

File # [redacted] Date dictated 05/10/01

by SA [redacted]

13 [redacted] 05.302

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/14/2001

[redacted] FINANCIAL EXECUTIVES INTERNATIONAL, 10 Madison Avenue, Morristown, New Jersey 07960, telephone number [redacted] was telephonically interviewed. After being advised of the identity of the interviewing Agent and the nature of the interview he provided the following information. b6 b7C

[redacted] contacted the FBI on 5/4/2001 to advise that on that day between 8:15 a.m. and 8:30 a.m. the main page and a seldom used secondary page of the web site of his company, FINANCIAL EXECUTIVES INTERNATIONAL (FEI), had been defaced. The defacement of the site, located at the URL www.FEI.org, consisted of anti-American language and symbols supporting the Chinese, including photographs of Communist leaders and a message of support by Ukrainian/Russian/Belarussian hackers. The defacement was signed "tty0", "Microfobia Group/GMF Team", and "Zenienss Uniao Hacker". Greetings were sent out to "SUB-SYS", "GMF", "f4nt4sy", "C0BR4S T34M, "ZUH", "[P(\)W], and "AHB". Some of the defacement is written in Spanish and references Brazil.

FEI hosts its own web page from a Windows NT operating system. [redacted] believes the page was compromised through an FTP password vulnerability. b6 b7C

The original FD-71 complaint form and original interview notes, as well as a 3.5" diskette containing computer logs and copies of the defaced pages are enclosed in the attached 1A envelopes.

Investigation on 05/09/2001 at Somerset, New Jersey (telephonically)

File # [redacted] Date dictated 05/14/2001 b3 b6 b7C

by SA [redacted] b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/14/2001

[redacted] JANOME-AMERICA, INC., 10 Industrial Avenue, Mahwah, New Jersey 07430, telephone number 973/825-3200, ext. [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, she provided the following information. b6 b7C

[redacted] filed an on-line report with the National Infrastructure Protection Center Watch and Warning Unit on 05/04/2001 regarding a compromise of her company's web site. In a follow-up conversation, she advised that on 05/03/2001 between 7:00 p.m. and 11:00 p.m. an unknown individual overwrote two pages of the company's web site with the following: "F*&k USA Government, f*$k PoizonBOx, contact:sysadmcn@yahoo.com.cn". The IP addresses of the two overwritten JANOME pages are 12.44.51.3/NFUSE and 12.44.51.4/NFUSE. Both IP addresses are behind a recently installed firewall and are assigned to pages remote users log on to obtain access to the company's internal networks. [redacted] was not sure what exploit was used to compromise the web page, but suspected it may have been through an open port. There did not appear to be any additional damage to the site, nor did it appear that the internal networks had been accessed. b6 b7C

A copy of the intrusion report forwarded by NIPC, as well as a 3.5" diskette containing logs and other files related to the intrusion which were provided by [redacted] are enclosed in the attached 1A envelopes. b6 b7C

Investigation on 05/10/2001 at Somerset, New Jersey (telephonically) b3

File # [redacted] Date dictated 05/14/2001 b6 b7C b7E

by SA [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] NOURISON, 5 Sampson Street, Saddle Brook, New Jersey [redacted] was advised the identity of the interviewing agent and the nature of the investigation. [redacted] b6 b7C then provided the following information:

[redacted] said that NOURISON's web page was replaced on Saturday, Sunday and Monday, May 5 through the 7th, 2001. [redacted] said that his page was one of the many being defaced as a result of the Solaris server worm exploit initiating the attack. [redacted] b6 b7C webpage had anti USA Government remarks and was part of the ongoing China-USA hacking conflict. As a result, [redacted] made the necessary system patches to eliminate the security holes. [redacted] said there was no loss of data or significant manual labor charges as a result of the defacement. [redacted] was able to restore the site from backups.

[redacted] said that he would send logs of the incident that b6 b7C were received by FBI Newark on May 9, 2001. A copy of the log has been placed in the file.

Investigation on 05/09/01 at Somerset, New Jersey (telephonically)

File # [redacted] Date dictated 05/10/01

by SA [redacted] b3 b6 b7C b7E

130 [redacted] 03,302

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/21/2001

[redacted] PICATINNY FEDERAL CREDIT UNION, 100 Mineral Springs Drive, Dover, New Jersey 07801, telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, he provided the following information. b6 b7C

[redacted] had previously submitted a Cyber Threat and Computer Intrusion Incident Report to the National Infrastructure Protection Center Watch and Warning Unit. The purpose of this interview was to follow-up on the information in his report.

[redacted] advised that between 7:45 p.m. on 5/13/2001 and 8:00 a.m. on 5/14/2001, one of their non-public web pages, springer.picatinnycu.org, was defaced with references to "Poison Box". Review of computer logs indicated the defacement originated from the IP address 202.195.100.2 and occurred as a result of either a vulnerable IIS server or the "sadmin" worm virus. Although the springer.picatinnycu.org server is connected to an internal network, there appeared to be no further damage beyond that of the web page. b6 b7C

A copy of the Cyber Threat and Computer Intrusion Incident Report sent to the National Infrastructure Protection Center Watch and Warning Unit is enclosed in the attached 1A envelope.

Investigation on 05/18/2001 at Somerset, New Jersey (telephonically) b3

File # [redacted] Date dictated 05/21/2001 b6 b7C b7E

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/04/2001

[redacted] RAO.com, 392 Atwood Place, Wyckoff, New Jersey 07481, telephone number 201/652-1500 ext. [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview he provided the following information. b6 b7C

[redacted] advised that his web site, www.RAO.com is used to market and sell framed artwork his company manufactures. RAO.com is a government contractor and the web site has a link to the Government Services Administration web site. The severs for this site are located in Hartford, Connecticut. On 05/25/2001 between 7:00 a.m. and 7:15 a.m. the web site was defaced with references to "Fuck USA government" and "PoizonBox". [redacted] stated the web site only has been up for about one week and took about 65,000 hours of programming. They did not have any logs available, but had a backup of the site and used that to replace the defaced page without any loss of business. b6 b7C

Investigation on 05/25/2001 at Somerset, New Jersey

File # [redacted] Date dictated 06/04/2001

by SA [redacted]

b3 b6 b7C b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] SCREENZONE MEDIA NETWORKS, 18 S. Orange Avenue, South Orange, New Jersey [redacted] was advised the identity of the interviewing agent and the nature of the investigation. [redacted] then provided the following information: b6 b7C

[redacted] said that SCREENZONE's web page was replaced on Saturday, Sunday and Monday, May 5 through the 7th, 2001. The first two attacks occurred at 17:48 and the third attack occurred at 21:48, respectively. [redacted] said that his page was one of the many being defaced as a result of the Solaris server worm exploit initiating the attack. [redacted] webpage had anti USA Government remarks and was part of the ongoing China-USA hacking conflict. As a result, [redacted] made the necessary system patches to eliminate the security holes. [redacted] said there was no loss of data or significant manual labor charges as a result of the defacement. [redacted] was able to restore the site from backups. b6 b7C

[redacted] explained that a batch file copied the cmd.exe file to root.exe, whereby when the root.exe was run in DOS, the website was updated with the defaced webpages. b6 b7C

[redacted] said that he would send logs of the incident that were received by FBI Newark on May 9, 2001. A copy of the log has been placed in the file.

Investigation on 05/09/01 at Somerset, New Jersey (telephonically) b3

File # [redacted] Date dictated 05/10/01 b6 b7C

by SA [redacted] b7E

130 [redacted] 02 302

#1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/14/2001

[redacted] SOFTWARE PLUS, INC., 25B Hanover Road, Florham Park, New Jersey 07932, telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, he provided the following information. b6 b7C

[redacted] contacted the FBI on 5/10/2001 and advised his company's web site, located at the IP address 62.236.17.2, had been defaced on 05/06/2001, 05/09/2001, and later advised it was defaced again on 5/12/2001. The defacement, which originated from IP address 199.38.132.12, consisted of the following message: "fuck USA Government, fuck PoizonBOx, contact: sysadmcn@yahoo.com.cn". There was no additional damage. SOFTWARE PLUS hosts its own web page on a server running Windows 2000. [redacted] did not know how the attackers were able to penetrate the web site. b6 b7C

The original FD-71 and a 3.5" diskette containing log files provided by [redacted] are enclosed in the attached 1A envelopes. b6 b7C

Investigation on 5/10/2001 at Somerset, New Jersey (telephonically) b3 b6 b7C b7E

File # [redacted] Date dictated 5/14/2001

by SA [redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] TRIANGLE MANUFACTURING, 116 Pleasant Avenue, Upper Saddle River, New Jersey 07458, [redacted] was advised the identity of the interviewing agent and the nature of the investigation. [redacted] then provided the following information: b6 b7C

[redacted] said that two files on TRIANGLE's web page was replaced with "Fuck US Government" and was part of the many webpages being defaced in the ongoing China-USA hacking conflict. As a result, [redacted] made the necessary system patches to eliminate the security holes replaced the webpage from backups and incurred no loss. [redacted] said that he did not have any logs of the incident and no additional information.

Investigation on 05/09/01 at Somerset, New Jersey (telephonically)

File # [redacted] Date dictated 05/10/01

by SA [redacted] b3 b6 b7C b7E

b3
b7E

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/10/2001

[redacted] US MORTGAGE CORPORATION, 19 Chapin Road, Pine Brook, New Jersey 07058, (973) 244-7100, ext [redacted] was advised the identity of the interviewing agent and the nature of the investigation. [redacted] then provided the following information: b6 b7C

[redacted] said that US MORTGAGE's web page was replaced on Sunday May 5th, 2001. [redacted] said that his page was one of the many being defaced as a result of the Solaris server worm exploit initiating the attack. [redacted] webpage had anti USA Government remarks and was part of the ongoing China-USA hacking conflict. As a result, [redacted] made the necessary system patches to eliminate the security holes. [redacted] said there was no loss of data or significant manual labor charges as a result of the defacement. [redacted] was able to restore the site from backups. b6 b7C

[redacted] said that he would send logs of the incident that were received by FBI Newark on May 9, 2001. A copy of the log has been placed in the file. b6 b7C

Investigation on 05/09/01 at Somerset, New Jersey (telephonically) b3 b6 b7C b7E

File # [redacted] Date dictated 05/10/01

by SA [redacted]

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases UNSUB	Character of case
	Complainant ☐ Protect Source [redacted] Tanglize Incorporated b6 b7C
	Complaint received ☐ Personal ☒ Telephonic Date 06/05/2001 Time 1730
Address of Subject UNKNOWN - Internet address	Complainant's address and telephone number 210 William Street Boonton, NJ 07005
	Complainant's DOB [redacted] / Sex: male

Subject's Description

Race: unk	☒ Male	Height: unk	Hair: unk	Build: unk	Birth date and birth place: unk-poss middle eastern
Age: unk	☐ Female	Weight: unk	Eyes: unk	Complexion: unk	Social Security Number: unk
Scars, marks and other data: unk					

Employer: unknown — Address — Telephone: unknown

Vehicle Description: none

Facts of Complaint

[redacted] of Tanglize Inc. called the duty agent to report an Internet hacker. Tanglize Inc. designs and hosts web sites for companies and is located in Boonton, New Jersey. Recently complainant has noticed statements against the US government, however, the have not been threats to this point. The messages that were posted, but did not appear on the web site, stated "F... the United States government." [redacted] feels that since his service is on an NT system the hacker is using an ASP function to place files on his server. Recently [redacted] has placed patches on his site that has temporarily blocked this person from accessing his site. Today just after 5 pm complainant received a phone call from a man with a heavy middle eastern or Indian accent. The man stated that he was his ISP, give me your E-Mail. Complainant asked for his name, his response was I am [redacted] Complainant has server logs with IP address of person hacking his site.

b6 b7C

Do not write in this space.

SA [redacted] (Complaint received by)

BLOCK STAMP

b3 b6 b7C b7E

[redacted]

Subject: Cyber Incident Report Form
Date: Fri, 11 May 2001 15:26:39 -0400
From: [redacted] b6 b7C
To: "nipc.watch@fbi.gov" <nipc.watch@fbi.gov>

Report date time=5/11/01 - 3:25 pm
Name=[redacted]
Title=network [redacted]
Telephone Fax Number=[redacted]201-489-6750
Email=[redacted]
Organization=goamerica communications corp.
Addrs_Street=433 hackensack avenue
City=hackensack
State=nj
Zip Code=07601
Country=usa
Question1_Organization=same
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=same
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=401 hackensack avenue, 4th floor
hackensack, nj 07601
Question3_Date_Time=5/11/01 - 6:46 am est and previous days
Question4_Critical=Yes
Question5_crit_infrasture=Telecommunications
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_other=
Question7_exp_problem=Yes
Question7_Remarks=we found that 2 of our windows nt 4.0 server running iis 4.0 (load balancing) had their default.htm/asp and index.htm/asp replaced. we discovered this on 5/10/01 and reinserted our regular page. on 5/11/01 at 6:46 am est, these 4 files were replaced again.
Question8_method_of_attack=Vulnerability exploited
Question8_method_of_attack=Unknown
Question8_Remarks=we found that these servers are not running the latest microsoft security updates, but we can't just throw them on without testing.
Question9_sus_perpetrators=Other
Question9_Remarks=seems to be part of the 'chinese attack' on us sites. a derogatory page towards the us gov't is put in place.
Question10_ip_addrs=
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=dell poweredge rack servers running windows nt 4.0 sp6 and iis 4.0
Question13_security_infrasture=Firewall
Question13_security_infrasture=Packet filtering
Question14_attack_loss_info=Unknown
Question14_Remarks=No Remarks
Question15_damage_systms=No
Question15_Remarks=No Remarks
Question16_what_actions=Other
Question16_what_actions=Log files examined
Question16_Remarks=we've tightened some of the ntfs security permissions, removed some unnecessary files and services. we're planning an upgrade to the latest security patches from microsoft (after testing).
Question17_Field Office=
Question17_fieldoff_inform=No

[redacted] b3 b7E

Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=5/11/01
Question19_org_work_update=internal
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=No additional remarks

FD-448 (Rev. 6-2-97)

FBI FACSIMILE

COVER SHEET

b6
b7C

PRECEDENCE

- ☐ Immediate
- ☒ Priority
- ☐ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☒ Unclassified

Time Transmitted: _____
Sender's Initials: _____
Number of Pages: 3
(including cover sheet)

To: Newark
Name of Office

Date: 05/11/2001

Facsimile Number: 973-792-3035

Attn: SSA [redacted]
Name Room Telephone

b6
b7C

From: NIPC Watch
Name of Office

Subject: Cyber Incident Report

Special Handling Instructions: _____

Originator's Name: NIPC Watch Telephone: 202-323-3205

Originator's Facsimile Number: _____

Approved: _____

Brief Description of Communication Faxed: _____

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/13/2001

The Geektools.com public Internet website was queried to determine the registration for the following Internet Protocol (IP) addresses:

208.177.103.98
211.136.17.141
202.241.213.160
133.38.151.20

The following represents the results of these queries:

IP Address	Registration Information
208.177.103.98	Concentric Network Corporation 1400 Parkmoor Avenue San Jose, California 95126
211.136.14.141	China Mobile Communications Corporation
202.241.213.160	C-Live Henseikyoku
133.38.151.20	Japan Network Information Center Fuundo Bldg. 3F, 1-2 Kanda-Ogawamachi, Chiyoda-ku Tokyo, 101-0052, JP

The print-outs containing more detailed information will be maintained within the Exhibit Section of the investigative file.

It should be noted that the aforementioned IP addresses were obtained from [redacted] Eligibility Services, Incorporated (ESI), 4144 North Central Expressway, Suite 210, Dallas, Texas, 75204 who, in turn, obtained the addresses from ESI's computer logs after ESI's web pages were defaced during the month of May 2001. b6 b7C

Investigation on 06/13/01 at Dallas, Texas

File # [redacted] Date dictated 06/13/01 b3 b6 b7C b7E

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/12/2001

[redacted] also known as [redacted] [redacted] Eligibility Services, Incorporated (ESI), 4144 N. Central Expressway, Suite 210, Dallas, Texas, 75201, telephone number [redacted] cellular telephone [redacted] born [redacted] Social Security Account Number [redacted] was advised of the identity of the interviewing agent and the purpose of the interview. [redacted] then provided the following information: b6 b7C

[redacted] has been employed with ESI as the System Engineer for approximately [redacted] He was responsible for addressing the problems resulting from the intrusion of ESI's computer system which occurred on May 7, 2001 and May 8, 2001. ESI is a company which provides technical consulting to businesses in the health industry. Part of its responsibilities includes developing databases for these companies.

[redacted] described the company's network system through the use of a diagram he provided. The webservers which were victimized on May 7, 2001 and May 8, 2001, use the Windows NT. 4.0 operating system with IIS 4.0 software and are labeled on the diagram as "ESIPDCDALLAS" and "WEBSERVER". The two Internet addresses handled under the ESIPDCDALLAS server are www.esinetwork.com which is the main site and contains the corporate web page and www.mail.esinetwork.com , which is the employee Internet mail network. The Internet mail network is strictly for employees to access their E-mail. The server listed as WEBSERVER on the diagram handles the following Internet sites: b6 b7C

1. www.northtexasviperclub.com This is sponsored by ESI's [redacted] and pertains to a club involving certain sports such as car racing.

2. www.texastrathlon.com: This is a similar club sponsored by ESI's [redacted] b6 b7C

3. www.hauk-i.com This is a website which was recently turned over to another company but was still being operated by ESI when the defacements occurred.

SERIALIZED/UPLOADED BY DL
W/TEXT
W/O [redacted]

164 [redacted] 01.302

Investigation on 06/07/01 at Dallas, Texas b3 b6 b7C b7E

File # [redacted] Date dictated 06/12/01

by SA [redacted]

4. www.ljbb.com : This is ESI's investment site which provides the public with information regarding investment opportunities.

5. www.medica-inc.com This is a site which once provided medical information and is no longer operational. ESI had no specific operational use for this site, and thus, once the intrusion occurred, ESI removed the site.

6. www.lopeznet.com This is another site operated by ESI. [redacted] b6 b7C did not provide additional information regarding this site.)

The servers contain some corporate sensitive information to include some financial data of the company which is restricted to specific individuals. The web pages displayed to the users do not have a logon banner with the exception of the employee E-mail site.

The network has a firewall (Watch Guard Firebox) as part of its security. The two servers mentioned above are under lock and key at all times and only three employees have access to the room where the server is stored. Only three employees have remote access to the network. Approximately 400 employees can access their E-mail through the Internet.

The following represents the events which occurred shortly before, during, and after the web page defacement:

On May 7, 2001, [redacted] became aware of the intrusion after b6 b7C several employees attempted to retrieve their E-mail and noticed their web page had been defaced. [redacted] also received several calls from vendors and clients who contacted him to advise him of defacements to ESI's public websites.

The defacements contained the words, "fuck USA Government" along with other information. [redacted] provided a compact b6 b7C disc (CD) which contains a copy of the defacement.

(SA [redacted] showed [redacted] copies of the web pages of www.ljbb.com captioned LJBB Investment Group, LP; www.texastriathlon.com captioned TexasTriathloncom; and www.northtexasviperclub.com captioned North Texas Viper Club. [redacted] confirmed that the web pages represented some of ESI's web pages which were defaced.) Based on a review of the computer logs,

[redacted] determined that the defacements occurred several times during May 7, 2001 and May 8, 2001. [redacted] copied the logs on the aforementioned CD. The CD also contains the script used by the intruder. b6 b7C

[redacted] has no indication that the intruder accessed the information on the servers. [redacted] noticed, however, that some of the log files were infected by a virus, PEARL SADMIND WORM. He opened the files under the Word Program and saved them as Word documents. [redacted] does not believe any other files were infected. [redacted] has applied patches to the system to avoid any further similar intrusions.

Based on the review of the logs, four Internet Protocol (IP) addresses of the intruder were captured on the logs. [redacted] conducted a trace route of these addresses on May 8, 2001. The results indicated that the IP addresses correspond as follows: b6 b7C

1. 208.177.103.98 XO Communications, Georgia ISP
2. 211.136.17.141 Net Plus, Hong Kong ISP
3. 202.241.213.160 C-Live, Japanese ISP
4. 133.38.151.20 Sai Tama University, Japan

[redacted] has monitored the firewalls to ensure there are no abnormalities. [redacted] has not noticed any major port scanning after May 8, 2001. b6 b7C

Approximately 20 hours of repair were conducted because of the intrusions. The financial loss to the company resulting from the web page defacements is estimated at $4,000.00. (20 hours @ $200.00 per hour.) A letter containing the breakdown of this figure is contained within the aforementioned CD.

The following items will be maintained within the Exhibit section of the investigative file:

1. Diagram of the network system provided by [redacted] b6 b7C
2. One CD containing copies of the logs, web page defacement, and the aforementioned letter.
3. Copy of the original web pages shown to [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/13/2001

The Geektools.com public Internet website was queried to determine the registration for the following Internet Protocol (IP) addresses:

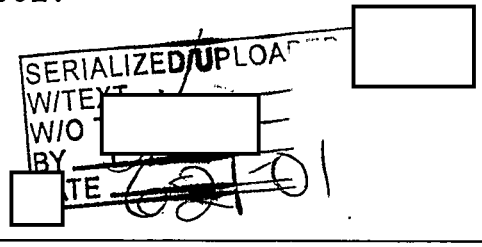
216.221.210.134
159.121.129.55
211.101.145.202
146.155.1.15

The following represents the results of these queries:

IP Address	Registration Information
216.221.210.134	Maxlink Communications Inc. 1 Yonge Street Suite 2415M5E1E5, CA
159.121.129.55	State of Oregon, Department of Administrative Services, 550 Airport Rd., Salem, OR 97310
211.101.145.202	HCINT Room 907 Building C, TianYin Tower No.D2 South Avenue FuXingMen Beijing, CN
146.155.1.15	SECICO Vicuna Mackena 4860 Santiago, Chile 6904411

The print-outs containing more detailed information will be maintained within the Exhibit Section of the investigative file.

It should be noted that the aforementioned IP addresses were obtained from [redacted] Richmont, 17855 Dallas Parkway, Dallas, Texas, 75240, who, in turn, obtained the addresses from Richmont's computer logs after Richmont's web pages were defaced during the month of May 2001. b6 b7C



Investigation on 06/13/01 at Dallas, Texas

File # [redacted] Date dictated 06/13/01

by SA [redacted]

b3 b6 b7C b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/6/2001

[redacted] Richmont, 17855 Dallas Parkway, Dallas, Texas, 75240, telephone number [redacted] born [redacted] Social Security Account Number [redacted] was advised of the identity of the interviewing agents and the purpose of the interview. [redacted] then provided the following information: b6 b7C

[redacted] has been employed as the Network Analyst for Richmont for approximately [redacted] is responsible for Richmont's infrastructure. Richmont is a marketing-focused merchant bank.

[redacted] described the company's network system through the use of a diagram he provided. The webserver which was victimized on May 5, 2001 through May 14, 2001 uses the Windows 2000 operating system with IIS 5.0 software and is labeled on the diagram as the ISA Server. The server contains Richmont's web page and receives e-mail as well. [redacted] does not consider any of the information on the server to be classified. At the time of the attacks, the web page did not have a logon banner warning unauthorized users not to enter. [redacted] however, has since installed a logon banner. The website is designed so anyone can log on. Passwords are required for employees to enter the other servers depicted on the schematic. b6 b7C

The network has a firewall installed as part of their security which is handled by a third party, AT&T. The web server is under lock and key at all times and only two or three employees have access to the room where the server is stored. There are 250 user workstations. Approximately 100 employees have remote access to the network. In order to access the system remotely, the employees must go through the AT&T security. As long as their Internet Protocol (IP) address falls within a specific range, the employee is authorized to enter.

During the time period May 5, 2001 - May 14, 2001, the Richmont web page experienced defacements. Based on a review of the network logs by [redacted] the following represents the dates, times and IP addresses from which the computer intrusions occurred: b6 b7C

SERIALIZED/UPLOADED BY DL

170 [redacted] 03.302

Investigation on 06/01/01 at Dallas, Texas

File # [redacted]

Date dictated 06/07/01

by SA [redacted]

b3 b6 b7C b7E

[redacted] b3 b6 b7C b7E

Date	Time	IP Address
5/5/01	7:13 P.M.	216.221.210.134
5/8/01	4:22 A.M.	159.121.129.55
5/12/01	8:15 A.M.	211.101.145.202
5/14/01	2:40 A.M.	146.155.1.15

[redacted] conducted a trace route command from the Disk Operating System (DOS) line on May 17, 2001 for all the aforementioned IP addresses and was only successful in tracing 146.155.1.15 to Leonera.puc.cl. [redacted] believes this is a site in China. b6 b7C

On May 21, 2001, at approximately 3:48 P.M., an unsuccessful intrusion attempt was made from IP address 61.156.28.14. This occurred after [redacted] had rebuilt the server. (Richmond's old IP address was 206.104.102.32, and the new IP address is 209.39.241.33.) On May 25, 2001, another unsuccessful attempt was made. [redacted] commented, however, that this last port scan may have been him testing the system.

Based on his research, [redacted] believes the intruder entered through port 80 of the router and placed the following two files throughout the system: b6 b7C

default.htm
default.asp

This resulted in the web page defacement. Although [redacted] did not maintain a copy of the defacement, he remembers it read something to the effect of "Fuck US Government Fuck USA" b6 b7C

[redacted] does not believe any further damage occurred to the system. He does not believe any of the additional servers of the network were affected. [redacted] scanned the entire machine and noted that nothing had been modified. The latest patch installed in the system was on May 15, 2001 which was patch Q293826. b6 b7C

(SA [redacted] showed [redacted] a copy of the web page of www.richmont.com captioned WELCOME TO RICHMONT. [redacted] confirmed that the webpage represented the company webpage which was defaced.) [redacted] provided logs pertaining to the intrusions listed above. SA [redacted] showed [redacted] a copy of a Cyber Incident Report which was sent to nipc.watch@fbi.gov. [redacted] confirmed he

had completed the report and sent it to the nipc.watch@fbi.gov Internet site.

[redacted] provided the interviewing agents with a letter which notes the financial loss to the company resulting from the web page defacement as being $145.00. The letter contains a breakdown of this figure. [redacted] also provided a portion of the logs pertaining to the intrusions set forth above. After beginning to print the logs, he realized the logs would be voluminous and decided to copy the logs onto a floppy disk. [redacted] provided the disk containing the log files.

b6
b7C

[redacted] added that his personal computer at home had also experienced a similar intrusion. [redacted] system is an entirely different and unrelated system. The intrusion into his personal computer occurred on May 7, 2001 at approximately 6:36 A.M. from IP address 140.126.139. [redacted] home IP address is [redacted]. [redacted] noted the same exact method of intrusion was utilized. [redacted] home address and telephone number are [redacted] His work station consists of a desk top and a lab top. [redacted] provided a copy of the logs for the intrusion of his personal computer. He indicated that the aforementioned disk also contained a copy of these logs as well.

b6
b7C

The following items will be maintained within the Exhibit section of the investigative file:

Diagram of the network system provided by [redacted]
Copy of the logs provided by [redacted]
Floppy disk provided by [redacted]
Letter containing financial loss provided by [redacted]
Copy of the original webpage shown to [redacted]
Copy of the Cyber Incident Report shown to [redacted]

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/19/2001

The Geektools.com public Internet website was queried to determine the registration for Internet Protocol (IP) address 202.107.11.78. According to the query, the address is registered to CHINANET-LN, A12, Xin-Jie-Kou-Wai Street, China.

The print-outs containing more detailed information will be maintained within the Exhibit Section of the investigative file.

It should be noted that the aforementioned IP address was obtained from [redacted] American Hallmark Group, 14651 Dallas Parkway #900, Dallas, Texas, who in turn, obtained the address from the business computer logs after its web pages were defaced during the month of May 2001. b6 b7C

b3 b6 b7C b7E

[redacted] 302

Investigation on 06/19/01 at Dallas, Texas

File # [redacted] Date dictated 06/19/01

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/07/2001

[redacted] American Hallmark Group, 14651 Dallas Parkway #900, Dallas, Texas 75240, provided one compact disc (CD) as she was instructed to do by [redacted] According to a note inside the case of the CD, the CD contained log files pertaining to a website defacement which occurred on May 5 and May 6, 2001, as well as a copy of the actual defacement. b6 b7C

The CD was placed within the (1A) exhibit section of the investigative file.

(X)

[redacted] b6 b7C

SERIALIZED/UPLOADED BY DL
W/TE [redacted]
W/O
BY [redacted]
TE 6/21/01

1 5 8 [redacted] U 2. 302

b3 b6 b7C b7E

Investigation on 06/06/01 [redacted] Dallas, Texas

File # [redacted] Date dictated 06/07/01

by SA [redacted]

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/07/2001

[redacted] American Hallmark Group/Hallmark Financial Services, 14651 Dallas Parkway #900, Dallas, Texas, telephone number 972-934-2400 extension [redacted] born [redacted] Social Security Account Number [redacted] was advised of the identity of the interviewing agents and the purpose of the interview. [redacted] then provided the following information: b6 b7C

[redacted] has been employed the with American Hallmark Group for approximately [redacted] She has been responsible for [redacted]

[redacted] described the company's network system through the use of a diagram she provided. The webserver which was victimized on May 5, 2001 and May 6, 2001, uses the Windows NT. 4.0 operating system with IIS 4.0 software and is labeled on the diagram as the NetFinity Server. The server contains client information and is utilized by American Hallmark Group employees to query their clients' accounts.. Information from the AS400 server listed on the diagram is downloaded into the NetFinity server. The webpage displayed to the employees does not have a logon banner warning unauthorized users not to enter. b6 b7C

Other servers listed on the lower right-hand side of the diagram are the following:

1. Server1- Novell server, contains financial accounting
2. Server2- NT server, manages log-ins
3. Server3- Novell server, premium finance program
4. AS400 - Runs all insurance functions

The network has a firewall installed as part of their security. The webserver is under lock and key at all times and only a few employees have access to the room where the server is stored. The router depicted in the diagram is an Intel Router. SA [redacted] viewed the router and noted model number ER 9525U.) Although there is no set security/procedural plan, all employees access their computers by using passwords. There are 100 user workstations with a total of 125 workstation capabilities. b6 b7C

170 [redacted] 02-302 b3

Investigation on 06/06/01 [redacted] Dallas, Texas b6 b7C b7E

File # [redacted] Date dictated 06/07/01

by SA [redacted]
SA

[redacted] b3 b6 b7C b7E

Only one employee has remote access to the network. E-mail for the company is handled externally through Ash Web Hosting.

The following represents the events which occurred shortly before, during, and after the webpage defacement:

On Saturday, May 5, 2001, [redacted] arrived at the office and read an e-mail from her supervisor who advised that there had been an intrusion into the America Hallmark Group's computer system. [redacted] noticed the company's webpage had been defaced. [redacted] provided the interviewing agents with a copy of the webpage defacement which reads as follows: b6 b7C

"fuck USA Government"
fuck PoizonBOx
contact:sysadmen@yahoo.com.cn"

(SA [redacted] showed [redacted] a copy of the webpage of www.hallmarkgrp.com captioned HALLMARK FINANCIAL SERVICES, INC. [redacted] confirmed that the webpage represented the company webpage which was defaced.) Based on a review of the computer logs, [redacted] approximated the time of the first intrusion to have occurred at 4:00 A.M. on May 5, 2001. The defacement occurred once again on the following day. [redacted] advised she does not currently have logs for May 6, 2001. [redacted] provided logs pertaining to May 5, 2001. SA [redacted] showed [redacted] a copy of a Cyber Incident Report which was sent to nipc.watch@fbi.gov. [redacted] confirmed she had completed the report and sent it to the nipc.watch@fbi.gov Internet site. b6 b7C

[redacted] believes the intruder entered the system through port 80 which is not blocked by the firewall. [redacted] has no indication that the intruder accessed the information on the server. The server contains personal information on the insured clients. [redacted] is not sure if any additional damage occurred other than the web defacement. b6 b7C

Based on the review of the logs, the Internet Protocol (IP) address which appears suspicious to [redacted] is 202.107.11.78. [redacted] conducted a trace route on this address through the DOS prompt. The results indicated that the IP address is that of Chinanet - China Telecom.

The Windows NT Operating System was upgraded, and approximately two weeks ago, patches were installed in the system

[redacted] b3 b6 b7C b7E

to avoid the vulnerability identified. The firewalls are being monitored to ensure there are no abnormalities. [redacted] does not know if there were any additional intrusion attempts. b6 b7C

[redacted] provided the interviewing agents with a letter which notes the financial loss to the company resulting from the web page defacement as being $8,540.00. The letter contains a breakdown of this figure. [redacted] advised she would provide a copy of a compact disc (CD) with additional log files at a future date.

The following items will be maintained within the Exhibit section of the investigative file: b6 b7C

Diagram of the network system provided by [redacted]
Copy of the web defacement provided by [redacted]
Copy of the logs provided by [redacted]
Letter containing financial loss provided by [redacted]
Copy of the original webpage shown to [redacted]
Copy of the Cyber Incident Report shown to [redacted]

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/19/2001

To: Chicago **Attn:** SA [redacted]

From: Dallas
NIPC
Contact: SA [redacted] 214-999-2393

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: Hacker/Honker Union of China
Illinois Secretary of State-Victim
Computer Intrusion
04/03/2001

Synopsis: To set forth partial lead coverage.

b3
b7E

Reference: [redacted]

Enclosure(s): Enclosed for Chicago are the following items:

1. The original and one copy of an FD-302 reflecting the interview of [redacted] American Hallmark Group.
2. One 1-A envelope containing documents provided by [redacted] and the original agent notes.
3. The original and one copy of an FD-302 reflecting the receipt of a compact disc (CD) containing the logs for the intrusion of American Hallmark Group.
4. One 1-A envelope containing the CD with the American Hallmark logs.
5. The original and one copy of an FD-302 reflecting the [redacted]
6. One 1-A envelope containing [redacted] listed on #5 above.
7. The original and one copy of an FD-302 reflecting the interview of [redacted] Richmont.
8. One 1-A envelope containing the original agent notes, one floppy disk with logs, and other pertinent documents provided by [redacted]
9. The original and one copy of an FD-302 reflecting the [redacted]
10. One 1-A envelope containing [redacted] listed as #9 above.
11. The original and one copy of an FD-302 reflecting the

b6
b7C
b7E

170 [redacted] 26-EC

SERIALIZED/UPLOADED BY DL
W/TE [redacted]
W/O
BY [redacted]

b6
b7C

To: Chicago From: Dallas
Re: [redacted] 06/19/2001

b3
b7E

interview of [redacted] Eligibility Services, Inc.
12. One 1-A envelope with the original agent notes as well as documents and a CD provided by [redacted] containing the logs and other pertinent data.
13. The original and one FD-302 reflecting the [redacted]
14. One 1-A envelope containing [redacted] listed as #13 above.

b6
b7C
b7E

Details: For the information of Chicago, as set forth on the referenced communication, Dallas has received numerous complaints regarding Web site defacements which are related to captioned matter. Dallas is in the process of interviewing approximately 17 victims and obtaining the logs and other pertinent data regarding the intrusions. The enclosed FD-302s represent some of the interviews as well as additional follow-up. Dallas has noted that the victims interviewed to date have all experienced similar Web page defacements which read, "fuck USA Government fuck PoizonBOx contact: sysadmen@yahoo.com.cn ". All victim servers were utilizing the Windows Operating System with IIS software. The following is a general outline of those entities which have experienced this intrusion along with the suspicious IP addresses noted by the victims.

Entity	Contact person	Suspect IP Addresses
American Hallmark Group	[redacted]	202.107.11.78
Richmont		216.221.210.134 159.121.129.55 211.101.145.202 146.155.1.15
Eligibility Services, Inc.		208.177.103.98 211.136.17.141 202.241.213.160 133.38.151.20

b6
b7C

Dallas will continue forwarding results of interviews as well as logs and other pertinent information as it is obtained.

To: Chicago From: Dallas
Re: [redacted] 06/19/2001

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear

♦♦